Lecture 2

There are several important things to note about this example:

- Composing two symmetries is again a symmetry (we write composition like multiplication).
- Inverting a symmetry is again a symmetry (e.g., inverting r we get r^{-1}, and s is its own inverse).
- In the group D_3, we write composition multiplicatively, but $rs \neq sr$, so composition is an operation which is a bit like multiplication, but does not work the way we are used to.
- We said that D_3 contains *all* symmetries, but you might object that, for example, the product $r^2(r^2s)$ is not in the group. But

  $$r^2(r^2s) = r^3rs = \mathrm{Id}\, rs = rs \in D_3.$$

  Another example is

  $$(rs)(r^2s) = rsr^2s = r(rs)s = r^2s^2 = r^2\,\mathrm{Id} = r^2 \in D_3,$$

  where we have used the relation $sr^2 = rs$ we found above, together with $s^2 = \mathrm{Id}$.
- To describe the group D_3 completely, we only need r and s and three fundamental relations from which everything else follows. We write this as

  $$D_3 = \langle r, s \mid r^3 = \mathrm{Id}, s^2 = \mathrm{Id}, srs = r^2 \rangle.$$

  We say that D_3 is *generated* by r and s. These three relations were determined above.

One can go on and do the same analysis for the symmetries of a square. The group of symmetries here is called the dihedral group D_4. Similarly, for a regular n-gon, for $n \geq 3$, we get the dihedral group D_n. It turns out that

$$D_n = \langle r, s \mid r^n = \mathrm{Id}, s^2 = 1, srs = r^2 \rangle,$$

so the main difference is that in general we have n rotations. It also turns out that D_n consists of $2n$ elements in total, namely

$$D_n = \{\mathrm{Id}, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}.$$

2.1 The definition of group

So, what is a group, mathematically? It is a collection of objects (e.g., symmetries, functions, numbers, matrices, etc) such that we can combine two of them to get a third in the collection, and such that every object has an inverse. More precisely,

Definition 2.1. A set G is called a *group* if the following holds:

i) (Binary operation) For any two elements $x, y \in G$ there is a uniquely defined element $x * y = xy \in G$.

ii) (Associativity) For every three elements $x, y, z \in G$ we have $x(yz) = (xy)z$.

iii) (Identity) There exists an element $\mathrm{Id} \in G$ such that for every $x \in G$ we have $\mathrm{Id} * x = x * \mathrm{Id} = x$.

iv) (Inverses) For every $x \in G$ there is a $x^{-1} \in G$ such that $x * x^{-1} = x^{-1} * x = \mathrm{Id}$.

It is important to understand that the binary operation which we have denoted as multiplication does not have to have anything to do with ordinary multiplication. It can be any binary operation (for D_3 it was composition), such as normal addition. For example, the set of integers

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$$

is a group under the binary operation $+$. Let's check the conditions:

i) For any $a, b \in \mathbb{Z}$, we have $a + b \in \mathbb{Z}$.

ii) For any $a, b, c \in \mathbb{Z}$ we have $a + (b + c) = (a + b) + c$.

iii) We have $\mathrm{Id} = 0$ such that for every $a \in \mathbb{Z}$, $0 + a = a + 0 = a$.

iv) For every $a \in \mathbb{Z}$ we have $-a \in \mathbb{Z}$ such that $a + (-a) = (-a) + a = 0$.

So here $* = +$ and $\mathrm{Id} = 0$.

Note that the set of integers $\mathbb{Z}$ is not a group under normal multiplication, because if $* = \times$, then $\mathrm{Id} = 1$ and $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$, so the fourth condition fails.

We will now give several further examples of groups:

Example 2.2.

i) The set of rational numbers

$$\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$$

is a group under addition with $\mathrm{Id} = 0$. The subset

$$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\},$$

($\mathbb{Q}$ with the zero removed) is a group under multiplication, with $\mathrm{Id} = 1$ (we had to remove zero because it does not have a multiplicative inverse). Ditto for $\mathbb{Q}$ replaced by the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$.

ii) A vector space V is a group under addition (see Lecture 18 from last term) (but it also has scalar multiplication, which is not relevant for its group structure).

iii) The set of invertible matrices

$$\mathrm{GL}_n(\mathbb{C}) = \{A \in \mathrm{M}_n(\mathbb{C}) \mid \det A \neq 0\}$$

is called the *general linear group* over $\mathbb{C}$ (it could be over $\mathbb{Q}$ or $\mathbb{R}$ as well). It is a group under matrix multiplication with $\mathrm{Id} = I_n$, the identity matrix. The only thing to check is: 1) that if A and B have inverses, then so do AB (this is true because the inverse of AB is $B^{-1}A^{-1}$) and 2) that $A(BC) = (AB)C$ (which we take for granted here).